UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/715,350	11/17/2000	David Montgomery	0500.0003231	6328

23418 7590 09/07/2006

VEDDER PRICE KAUFMAN & KAMMHOLZ
222 N. LASALLE STREET
CHICAGO, IL 60601

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 09/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 09/715,350	**Applicant(s)** MONTGOMERY, DAVID	
	Examiner Michael J. Simitoski	**Art Unit** 2134	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 26 August 2006 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
 a) ☒ The period for reply expires 3 months from the mailing date of the final rejection.
 b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

 Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
 (a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);
 (b) ☒ They raise the issue of new matter (see NOTE below);
 (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
 (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

 NOTE: *See Continuation Sheet*. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☒ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
 The status of the claim(s) is (or will be) as follows:
 Claim(s) allowed: *39*.
 Claim(s) objected to: *3*.
 Claim(s) rejected: *1,2,4-7,12-17,19-21,24-33,35,37,38 and 40-46*.
 Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

Continuation of 3. NOTE: The amendment to the specification aims to change the scope and understanding of the software applications originally disclosed and therefore constitutes new matter, requiring further consideration. Further, it is noted that if the objection to the new matter were overcome and the amendment to the claims entered, the amended claims would be rejected under the same rationale as already applied in the final rejection.

Continuation of 11. does NOT place the application in condition for allowance because: Applicant's response (p. 16) argues that Samar in view of Menezes lacks the following:

Claim 4, "publishing the signed certificate set of certificate issuing units"
Claim 6, "wherein the step of collecting the at least one cross certificate includes collecting cross certificates from a data repository associated with the anchor CA"
Claim 7, "digitally sign the created signed certificate set to provide a trusted cross certificate signed certificate set for use by a client unit"
Claim 12, "regarding the plurality of signed certificate sets on a per anchor certificate issuing unit basis wherein each of the signed certificate sets contains the claimed information in publishing each signed certificate set as claimed,
Claim 14, "caching, by a client unit, a copy of the signed certificate set of certificate issuing units and wherein the client unit does not perform validation of the certificate issuing unit certificates but validates an end entity certificate by seeing if the certificate issuing entity associated with the end entity is on the cached signed certificate set and using the public key of that certificate issuing entity to validate the end entity certificate"
Claim 26, the claimed signed certificate set generator is claimed and the client unit.

Regarding claim 4, Samar, as modified, discloses publishing the signed certificate set of certificate issuing units (signed list) (col. 6, lines 35-36 & col. 7, lines 3-6).
Regarding claim 6, Samar, as modified, discloses wherein the step of collecting at least one cross certificate includes collecting cross certificates/list of certificates from a data repository/enterprise administrator (col. 5, lines 53-55 & col. 6, lines 15-21).
Regarding claim 7, Samar, as modified, discloses digitally signing the created signed certificate set (col. 6, lines 27-31) to provide a trusted cross certificate signed certificate set (signed list) for use by a client unit (col. 6, lines 35-37).
Regarding claim 12, Samar, as modified, creating a plurality of signed certificates sets (col. 6, lines 28-34) on a per anchor certificate issuing unit basis/enterprise administrator (col. 6, lines 36-37) wherein each signed certificate set contains at least a list of unique identifiers and associated public keys (certificates) of each certificate issuing unit/trusted certificate authority (col. 6, lines 14-21) trusted by an anchor certificate issuing unit/trusted certificate authority (col. 6, lines 14-21) and publishing each signed certificate set wherein each published signed certificate set is accessible by a plurality of different client units (col. 6, lines 35-36 & col. 7, lines 3-6). See also col. 8, lines 21-23).
Regarding claim 14, Samar, as modified, discloses caching, by a client unit (col. 6, lines 55-60), a copy of the signed certificate set of certificate issuing units trusted by the anchor certificate issuing unit (col. 6, lines 55-60) and wherein the client unit does not perform validation of certificate issuing unit certificates but validates an end-entity certificate by seeing if the certificate issuing entity associated with the end-entity is on the cached signed certificate set (col. 5, lines 58-61) and using the public key of that certificate issuing entity to validate the end-entity certificate (col. 2, lines 60-65 & col. 7, lines 34-36).
Regarding claim 26, Samar discloses a signed certificate set generator/enterprise administrator (col. 6, lines 28-34) to collect a plurality of cross certificates/list of certificates (col. 6, lines 14-21) associated with at least one anchor certificate issuing unit/enterprise administrator (col. 6, lines 14-21), and obtain a plurality of issuing unit public keys and associated unique identifiers (certificates) (col. 6, lines 28-34) for cross-certified certificate issuing units identified by a plurality of cross certificates/list of certificates (col. 6, lines 14-21) and operative to create a signed certificate set (col. 6, lines 28-34) identifying certificate issuing units/certificate authorities determined to be trusted by the anchor certificate issuing unit/enterprise administrator (col. 6, lines 14-21), based on cross certificates (enterprise administrator makes decision), wherein the signed certificate set includes at least a unique identifier and public key of each trusted certificate issuing unit and an associated digital signature (col. 6, lines 14-31) and at least one client unit/users in operative communication with the signed certificate set generator/enterprise administrator (col. 6, lines 36-37) and operative to access the signed certificate set and to determine whether a received message is from a trusted source based on the signed certificate set (col.. 2, lines 57-59) (the purpose of Samar's invention). Samar lacks explicitly collecting cross certificates (explicitly cross certificates) in creating the signed certificate set. However, Menezes teaches that a cross-certificate is a certificate created by one certification authority to certify the public key of another (p. 572, 13.39 Definition). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Samar to collect the enterprise administrator's cross-certificates to build the list of trusted CA's for use in the wallet. One of ordinary skill in the art would have been motivated to perform such a modification because a cross-certificate is a certificate created by one certification authority to certify the public key of another, as taught by Menezes (p. 572, 13.39 Definition).

Applicant's response (p. 17) argues that claims 16-17, 19-21, 24-29 & 38-44 constitute statutory subject matter in light of the amendments to the specification. However, these amendments are not entered because they raise the issue of new matter and require more than nominal consideration. The rejections under 35 U.S.C. §101 are maintained.

Applicant's response (p. 19) argues that there is not teaching of enterprise administrator cross certificates in Samar or Menezes and no motivation provided by the mere definition of a cross certificate. Applicant also argues that the motivation is a mere definition of a cross certificate and that Menezes merely defines what a cross certificate is which is known in the art. However, the Menezes reference is a well-known reference in the field of cryptography. Applicant's claimed subject matter is anticipated by Samar in that Samar's enterprise administrator collects certificates from whom he trusts and signs a set of these certificates, except that Samar is silent regarding how the enterprise administrator determines from where the certificates are drawn (col. 5, lines 53-56). However, Menezes teaches that a cross certificate, literally, certifies other certificate authorities public key. What makes a cross certificate different from a normal certificate is that rather than attesting to the public key of an end user, the cross certificate attests to the validity of a certificate authority's public key.

Therefore, one having an ordinary level of skill in the art in cryptography would have been motivated to use, as his particular mechanism to decide which certificates to add to the list, turned to the Menezes reference and hence turned to cross certificates, which serve the purpose of signifying to the certificate authority (enterprise administrator) that he trusts another certificate authority's public key. As Samar's invention needs to determine which trusted public keys are added to the list, one of ordinary skill would be motivated to turn to cross certificates to satisfy this very need.

Applicant's response (p. 19) also argues that the claims are allowable because there is only one enterprise administrator disclosed and the claims recite "created a plurality of signed certificate sets ...". However, Samar teaches publishing updated signed certificate sets (col. 8, lines 11-39). Further, if the claims explicitly stated that multiple signed certificate set generators existed, it is believe that one having ordinary skill in the art of computers would realize that more than one enterprise administrator of more than one enterprise would have been motivated to use Samar's invention, as modified by Menezes, for all the benefits disclosed in Samar and Menezes.

Applicant's response (p. 19) argues that the enterprise administrator in Samar "does not appear to be an anchor certificate issuing unit". However, as the enterprise administrator digitally signs data including a public key and identifier, a certificate of certificates, one of ordinary skill would identify the enterprise administrator as an anchor certificate-issuing unit.

JACQUES LOUIS-JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100